'Cybercrime vraagt om nog slimmere, zichzelf beschermende netten'

- Ilse Kleijne
- i.kleijne@energeia.nl

AMSTERDAM (Energeia) - Slimme oftewel digitale energienetten brengen het risico van cybercriminaliteit met zich mee. Het antwoord daarop? De netten moeten in de toekomst nog slimmer worden om cybercriminelen zo voor te blijven. Dat stellen Gerard van de Kamp en Eelco Stofbergen van IT-consultancybedrijf CGI.

Energiebedrijven moeten zich, als belangrijke doelwitten, niet alleen richten op het buiten de deur houden van cybercriminelen, zo betoogde voormalig topman Keith Alexander van de Amerikaanse veiligheidsdienst NSA onlangs. Volgens Alexander moeten zij zich nu met name gaan richten op het monitoren van hun eigen IT-systemen, zodat ze het sneller in de gaten hebben als cybercriminelen de beveiliging aan de digitale poort toch hebben weten te omzeilen en 'binnen' zijn gekomen met hun malware.

Die mening wordt gedeeld door vice-president *consulting services utilities* Gerard van de Kamp en *thougth leader cyber security* Eelco Stofbergen bij CGI. CGI onderzoekt momenteel voor het Agentschap Telecom wat de risico'skunnen zijn voor de Nederlandse maatschappij als het grootste deel van de huisaansluitingen tegen 2020 zijn voorzien van digitale gas- en stroommeters.
Op dat onderzoek mogen ze nu niet ingaan. Wel lichten ze toe hoe volgens hen het onderwerp cybersecurity inmiddels op de agenda staat van energiebedrijven. Uit een wereldwijde trendrapportage van CGI (zie kader) is volgens Van de Kamp en Stofbergen naar voren gekomen dat er sprake is van "een *mindshift*", aldus Van de Kamp. "Cybersecurity kwam eerder bij energiebedrijven in de top drie van belangrijke trends. Nu wordt het onderwerp niet meer als trend gezien, maar als iets waar gewoon aandacht wordt besteed."

Security officer
Dat heeft te maken met het feit dat de fysieke wereld van energienetten gekoppeld geraakt is aan IT, er daardoor allerlei data worden gegenereerd en de bedrijven steeds meer datagedreven zijn geworden, aldus Van de Kamp. "De energietransitie is de grote *game changer* voor de digitalisering van de netten." Stofbergen: "Het onderwerp is *business as usual* geworden, iets wat onderdeel is geworden van de reguliere bedrijfsvoering."
Dat 'business as usual' uit zich bijvoorbeeld in het feit dat energiebedrijven bijvoorbeeld iemand aanstellen in de functie van security officer, noemt Van de Kamp als voorbeeld. "Het is een structurele post aan het worden, waar budget voor wordt vrijgemaakt, met steun vanuit het management." Stofbergen: "Het zijn geen eenzame krijgers binnen een bedrijf meer."

Dat preventie niet alleen voldoende is, zoals Alexander betoogde, is volgens Stofbergen "al voldoende gebleken" door internationale hack-incidenten. "Vroeger waren bedrijven kastelen met grachten. Door de invoering van IT in systemen is alles met elkaar verbonden, afsluiten kan niet meer. Vroeger kon je bij wijze van spreken alleen schade aan de assets van de energiesector aanrichten met een bom. Door de digitalisering word je kwetsbaarder. Daarom is detectie nu cruciaal."

Schadebeperking
Energiebedrijven moeten zich inderdaad focussen op "wat als-scenario's", sluit Van de Kamp daarbij aan, en er in hun voorbereiding "vanuit gaan dat er iets gebeurt" in plaats van proberen te voorkomen dat er iets gebeurt. "Als de energie-infrastructuur wordt aangevallen, gaat de boel in Nederland plat. De schade moet beperkt blijven."
Detectie van eenmaal binnengedrongen hardware moet nu dus prioriteit zijn, beamen zij. Stofbergen: "De inzet daarvoor zal je de komende jaren zien groeien, en het detecteren zal beter worden. Daarna kan de focus weer worden verlegd naar de preventieve kant." Het is volgens hem bovendien wachten op "de volgende generatie slimme maatregelen".

200 dagen
Hij denkt dan aan "netwerken die zichzelf dynamisch kunnen configureren, om zichzelf zo te beschermen tegen een cyberaanval". "Dat is de volgende stap in de toekomst, voor nu is de aandacht voor detectie goed. Want er gebeurt meer dan we denken, en het duurt nu gemiddeld nog 200 dagen tussen het moment dat er foute software een systeem binnenkomt en dit wordt opgemerkt."
Stofbergen (voorheen werkzaam bij het National Cyber Security Centrum van de rijksoverheid) en Van de Kamp willen niet ingaan op de vraag of het telekwetsbaarheid-onderzoek rond slimme meters, waar Agentschap Telecom nu om heeft gevraagd, niet rijkelijk laat komt. Had dit niet uitgevoerd moeten worden voordat besloten werd tot een grootschalige uitrol van slimme meters bij kleinverbruikers?

"De techniek ontwikkelt zich. Daardoor kunnen risico's veranderen", geeft Stofbergen in het algemeen aan. "Dan moet je kijken of het beeld dat van de risico's bestaat, nog klopt. We zien dat de capaciteiten van aanvallers veranderen. Zo komen er meer statelijke actoren, dus hackers die door overheden worden gesponsord. Als aanvallers meer kunnen, veranderen de risico's."

Het is zaak dat er in Nederland wordt gekeken wat de vervolgstap moet worden op het gebied van cybercriminaliteit, denkt Stofbergen. Het is nog wachten op de wettelijke meldplicht van incidenten voor cruciale bedrijven (nu ter beoordeling in de Tweede Kamer). "Die wet is er primair op gericht op ondersteuning: de overheid helpt je als er iets gebeurt." Maar ook moet er binnen diverse sectoren afspraken worden gemaakt, stellen de twee. "Wat wil je aan maatregelen treffen om tot een minimum veiligheidsniveau te komen?"

Nederlandse bedrijven iets te tevreden met cyberinzet

Het vertrouwen dat Nederlandse bedrijven in hun eigen maatregelen tegen cybercriminaliteit hebben, loopt niet volledig in pas met de daadwerkelijke maatregelen. Dat is de conclusie van IT-dienstverlener en cybercrime-adviseur CGI op basis van een onderzoek dat het bedrijf heeft gehouden naar de mate waarin bedrijven zich bewust zijn van het risico op cybercriminaliteit. Voor het onderzoek sprak CGI met 965 leidinggevenden van bedrijven wereldwjd in tien sectoren (van nutsbedrijven tot onder andere financiën, zorg, transport, communicatie en overheid). Er deden 66 Nederlandse bedrijven mee.

Waar 53% van alle bedrijven wereldwijd er vertrouwen in heeft dat de eigen maatregelen tegen cybercriminaliteit op orde zijn, ligt dat percentage onder de Nederlandse bedrijven op 66%. Dat hogere Nederlandse vertrouwen kan volgens CGI samenhangen met het feit dat de Nederlandse overheid cybercrime mede-aanpakt, door wet- en regelgeving.

Dat het Nederlandse vertrouwen niet helemaal gerechtvaardigd is, heeft te maken met het feit dat de bedrijven die meededen aan het onderzoek sommige zaken juist minder goed op orden hebben dan internationaal het geval lijkt. Er zijn namelijk verschillende stappen die bedrijven moeten zetten, aldus CGI, zoals hun kritieke assets identificeren, een noodplan hebben voor incidenten en inzicht krijgen in de financiële risico's van een cyberaanval. Nederlandse bedrijven bleken tijdens het onderzoek minder vaak over een dergelijk plan te beschikken (in 55% van de gevallen, waar dat wereldwijd op 67% ligt), en minder vaak goed in het vizier hebben welke bedrijfsbezittingen aantrekkelijk voor hackers zijn (57% versus 67%).

CGI signaleert verder dat bedrijven in sectoren met hogere risico's op cyberaanvallen, zoals nutsbedrijven, olie- en gasbedrijven, financiële en overheidsinstallingen, een hogere prioriteit geven aan investeringen om cybercriminaliteit tegen te gaan. De belangsteling voor het verzekeren tegen cybercriminaliteit neemt ook toe.